

SCAMS

Tax Refund Scam Targets College Students and Staff

The IRS says there's a new phishing scam aimed at people with email addresses ending in ".edu."



Getty Images

Here's a new warning from the IRS: Watch out for an IRS-impersonation scam targeting people associated with colleges, universities, and other educational institutions – including students and staff – who have an ".edu" email addresses. The phishing emails appear to target university and college students from both public and private, profit and non-profit institutions.

The fraudulent emails display the IRS logo and use various subject lines such as "Tax Refund Payment" or "Recalculation of your tax refund payment." If you receive one of these emails, you'll be asked to click a link and submit a form to claim your refund. The fake website you'll be taken to will have you provide your:

- Social Security Number
- First Name
- Last Name
- Date of Birth
- Prior Year Annual Gross Income (AGI)
- Driver's License Number
- Current Address
- City
- State/U.S. Territory
- ZIP Code/Postal Code
- Electronic Filing PIN

Do NOT fall for this trick! If you receive this scam email, do not click on the link. Instead, immediately report it to the IRS by (1) saving the email using "save as" and (2) send that attachment to phishing@irs.gov.

If you already received the email and provided the requested information, you should go to the [IRS's website](#) and get an Identity Protection PIN right away. This six-digit number will help prevent identity thieves from filing fraudulent tax returns in your name.

Anyone who tries to e-file their tax return and has it rejected because a return with their Social Security number has already been filed should file a [Form 14039](#) to report the possible identity theft. See the IRS's [Identity Theft Central](#) website for more information about the signs of identity theft and actions to take.

Kiplinger

© 2021 The Kiplinger Washington Editors Inc.